mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message; and

(c) forwarding the non-executable format to the recipient of the e-mail message.

5. (Amended) The method of claim 4, wherein step (b) comprises:

(i) providing a plurality of sacrificial servers in communication with the gatekeeper server;

(ii) forwarding the attachment from the gatekeeper server to one of the plurality of sacrificial servers; and

(iii) converting the attachment to the non-executable format on said one of the plurality of sacrificial servers by using said one of the plurality of conversion processes selected in accordance with the type of the e-mail message, the non-executable format retaining the appearance, human readability and semantic content of the e-mail message.

9. (Amended) The method of claim 4, wherein step (b) comprises:

(i) maintaining a list of approved attachment file types and extensions;

(ii) determining whether the attachment is of a type or extension which is in the list of approved attachment file types and extensions; and

(iii) if the attachment is not of a type or extension which is in the list of approved attachment file types and extensions, informing the recipient that a message containing a non-approved attachment has been received.

16. (Amended) A system for protecting a network from a virus contained in an e-mail message as executable code, the system comprising:

a workstation computer on the network used by a recipient of the e-mail message;

a gatekeeper server, in communication with the workstation computer over the network,

for receiving the e-mail message; and

a computer on the network for converting the e-mail message from an executable format to a non-executable format by using one of a plurality of conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and forwarding the converted e-mail message to the workstation computer.

20. (Amended) The system of claim 16, wherein the computer for converting is one of a plurality of sacrificial servers which are in communication with the gatekeeper server.

21. (Amended) The system of claim 20, wherein the plurality of sacrificial servers are examined for virus activity.

22. (Amended) The system of claim 21, wherein the network further comprises a read-only device, and wherein the sacrificial servers are rebooted from a safe copy of an operating system obtained from the read-only device.

23. (Amended) The system of claim 20, wherein communications between the gatekeeper server and the sacrificial servers are authenticated using a challenge-and-response technique.

24. (Amended) The system of claim 16, wherein the network maintains a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, informs the recipient that a message containing a non-approved attachment has been received.

31. (Amended) A sacrificial server for use on a network, the sacrificial server comprising: